Amendments To Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1.   (Currently Amended) A <u>method, comprising:</u> ~~method for registering and using a proffered biometric sample for facilitating a Radio-Frequency (RF) transaction, said method comprising:~~

detecting <u>a</u> ~~said proffered~~ biometric sample at a biometric sensor <u>to create biometric sample data</u>;

associating said ~~proffered~~ biometric sample <u>data</u> with at least one of <u>a Radio Frequency (RF)</u> ~~an RF~~ device, a user identifier, <u>or</u> [[and]] a transaction account;

verifying said ~~proffered~~ biometric sample <u>data</u> ~~in order~~ to activate said RF device ~~and confirm said proffered biometric sample~~;

storing said ~~proffered~~ biometric sample as [[a]] registered biometric sample <u>data in response to said verifying said biometric sample data</u>;

receiving [[a]] transaction <u>biometric sample data associated with</u> ~~request from~~ said RF device, wherein said ~~transaction request comprises a~~ transaction biometric sample <u>data is further associated with a transaction request; and</u>~~; and,~~

<u>comparing</u> ~~authorizing said transaction request when~~ said transaction biometric sample <u>data to said registered biometric sample data to facilitate authorization of said transaction request</u> ~~matches said registered biometric sample~~.

2.   (Canceled)

3.   (Canceled)

4.   (Currently Amended) The method of claim 1, wherein said detecting [[of]] said ~~proffered~~ biometric sample <u>data</u> includes at least one of detecting, associating, <u>or</u> [[and]] processing ~~at least one~~ additional ~~proffered~~ biometric sample <u>data</u>.

5.   (Canceled)

6. (Currently Amended) The method of claim 1, wherein said verifying [[of]] said proffered biometric sample data comprises comparing said proffered biometric sample data with [[a]] stored biometric sample data.

7. (Currently Amended) The method of claim 6, wherein said comparing [[of]] said proffered biometric sample data with said stored biometric sample data includes comparing said proffered biometric sample data with at least one of [[an]] authorized biometric sample data or [[and]] unauthorized biometric sample data.

8. (Canceled).

9. (Currently amended) The method of claim 1, wherein said verifying [[of]] said proffered biometric sample data includes verifying said proffered biometric sample data using at least one of a protocol/sequence controller or [[and]] a third-party security vendor.

10. (Canceled).

11. (Currently Amended) The method of claim 1, wherein said storing [[of]] said proffered biometric sample data includes storing said proffered biometric sample data in [[on]] at least one of a local database, a remote database, or [[and]] a third-party controlled database.

12. (Currently Amended) The method of claim 1, wherein said verifying [[of]] said proffered biometric sample data comprises comparing said proffered biometric sample data with [[a]] verification biometric sample data received from said RF device.

13. (Currently Amended) The method of claim 1, wherein said biometric sensor comprises at least one of: a retinal scan sensor, an iris scan sensor, a fingerprint sensor, a hand print sensor, a hand geometry sensor, a voice print sensor, a vascular sensor, a facial sensor, an ear sensor, a signature sensor, a keystroke sensor, an olfactory sensor, an auditory emissions sensor, or [[and]] a DNA sensor.

14. (Currently Amended) The method of claim 1, wherein said proffered biometric sample comprises a biometric sample characteristic comprising at least one of: blood flow, correctly

3

aligned ridges, pressure, motion, body heat, ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore location, loops, whorls, or [[and]] arches.

15. (Currently Amended) The method of claim 1, wherein said user identifier comprises at least one of: personal information, financial information, loyalty point information, employee information, employer information, medical information, or and/or family information.

16. (Currently Amended) The method of claim 1, further comprising associating [[a]] second biometric sample data with at least one of a second RF device, a user identifier, or [[and]] a transaction account.

17. (Currently Amended) The method of claim 1, wherein said biometric sensor is associated with at least one of: a local database, a remote database, a portable storage device, a host system, an issuer system, a merchant system, a fob issuer system, an employer, a financial institution, a non-financial institution, a loyalty point provider, a company, the military, the government, a school, a travel entity, a transportation authority, or [[and]] a security company.

18. (Currently Amended) The method of claim 1, further comprising:

transmitting a device authentication code from a sample receiver to said RF device;

receiving an encrypted device authentication code, [[a]] second proffered biometric sample data, and a unique device identification code from said RF device;

decrypting said encrypted device authentication code using a unique device decryption key corresponding to said unique device authentication code;

comparing said decrypted device authentication code to said device authentication code; and

authenticating said RF device in response to when said second proffered biometric sample data matching matches said registered biometric sample data and in response to when said decrypted device authentication code matching matches said device authentication code.

19.   (Currently Amended) The method of claim 18, further comprising:

receiving an encrypted device account code from said RF device;

decrypting said encrypted device account code using said unique device decryption key; and

transmitting said decrypted device account code to facilitate an RF transaction. for processing.

20.   (Previously Presented) The method of claim 19, further comprising:

receiving a reader authentication code from said RF device;

encrypting said reader authentication code using a reader encryption key to create an encrypted reader authentication code; and

transmitting said encrypted reader authentication code to said RF device for authentication of said sample receiver.

21.   (Currently Amended) An authorized sample receiver (ASR), comprising: configured to register a biometric sample and facilitate a Radio Frequency (RF) transaction, said ASR comprising:

a biometric sensor configured to detect receive a first proffered biometric sample to create biometric sample data, wherein said biometric sample data is associated with at least one of an RF device, a user identifier, or a transaction account;

a communications device configured to receive a second proffered biometric sample associated with an RF device, wherein said ASR is configured to verify said second proffered biometric sample in order to activate said RF device, and wherein said ASR is database configured to store said first proffered biometric sample data as [[a]] registered biometric sample data in response to said ASR verifying said biometric sample data, wherein said ASR is configured to activate said RF device in response to said ASR verifying said biometric sample data when said second proffered biometric sample matches said first proffered biometric sample;

a communications device ~~an RF Identification (RFID) reader~~ configured to receive ~~a~~ ~~transaction request from said RF device, wherein said transaction request comprises a~~ transaction biometric sample data associated with said RF device, wherein said transaction biometric sample data is further associated with a transaction request~~, an encrypted device account code, and a~~ ~~unique device identification code~~;

~~a plurality of device-specific decryption keys;~~ and

an authentication circuit configured to ~~select a unique device decryption key from said~~ ~~plurality of device-specific decryption keys by associating said unique device identification code~~ ~~with said unique device decryption key, and wherein said authentication circuit is further~~ ~~configured to use said unique device decryption key to decrypt said encrypted device account~~ ~~code; and wherein said authentication circuit is further configured to~~ compare said transaction biometric sample data to said registered biometric sample data to facilitate authorization of said transaction request ~~in order to authenticate said RF device and facilitate said RF transaction~~.

22. (Currently Amended) The ASR of claim 21, wherein said transaction request further comprises an encrypted device account code and an RF device identification code ~~further~~ ~~comprising a USB interface configured to communicate with said RF device~~.

23. (Currently Amended) The ASR of claim 22, wherein said authentication circuit is further configured to select a device decryption key from a plurality of device-specific decryption keys by associating said RF device identification code with said device decryption key, and wherein said authentication circuit is further configured to use said unique device decryption key to decrypt said encrypted device account code to create a decrypted device account code ~~USB~~ ~~interface is further configured to personalize said RF device~~.

24. (Currently Amended) The ASR of claim 23 [[21]], wherein said decrypted device account code comprises a device account number in a magnetic stripe format configured to be transmitted to a Point of Sale (POS) device and processed under a ~~merchant's~~ business as usual standard for a merchant.

25. (Previously Presented) The ASR of claim 21, further comprising an RFID reader PIN interface configured to receive a secondary verification.

26. (Currently Amended) The ASR of claim 21, <u>wherein said communications device is</u> further configured to transmit a device authentication code to said RF device, receive an encrypted device authentication code from said RF device, and decrypt said encrypted device authentication code using said unique device decryption key in order to authenticate said RF device.

27. (Currently Amended) The ASR of claim 21, <u>wherein said communications device is</u> further configured to receive an ASR authentication code from said RF device, encrypt said ASR authentication code, and transmit said encrypted ASR authentication code to said RF device in order to facilitate authentication of said ASR.

28. (New) The ASR of claim 21, further comprising a USB interface configured to at least one of communicate with said RF device or personalize said RF device.